CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

4 APRIL 2017

(U) NATIONAL

(U) District of Columbia – WikiLeaks Releases More Information from CIA Breach
(U) Washington – WikiLeaks released another round of information from the recent hack of the CIA. The release includes alleged cyber and hacking tools from the CIA's "Marble Framework" which is used to hamper forensic investigators and anti-virus companies from tracking the origin of cyberattacks. The CIA would not comment on the authenticity of the released data, but a spokesperson said that the release was designed to harm or hamper the ability of US intelligence agencies to protect against terrorists and other adversaries.
SOURCE: 3 April 2017, FCW

(U) Maryland – Pro-ISIS Hacker Group Releases Kill List
(U) Bethesda – The United Cyber Caliphate (UCC) released a "kill list" containing the names and addresses of 8,786 Americans, and an accompanying video that also threatened President Trump, according to the Site Intelligence Group. Last July, the UCC released a list with more than 1,700 names, targeting members of Christian churches and Jewish synagogues in the US and urging followers to "kill them all."
SOURCE: 4 April 2017, International Business Times

(U) INTERNATIONAL

(U) Russia – Suspect in St. Petersburg Metro Blast Likely from Central Asia
(U) St. Petersburg – The suspect in Monday's attack on a subway train that killed 14 people and wounded 50 was probably perpetrated by a Russian citizen born in Kyrgyzstan and was identified as Akbarzhon Jalilov by the Kyrgyzstan security service. So far, no organization has claimed responsibility for the attack and although Russian officials said they were treating it as an act of terrorism, there has been no official confirmation of any link to Islamist radicals.
SOURCE: 4 April 2017, Reuters

(U) Monaco – International Athletic Organization Hacked by Russian Hacker Group
(U) Monte Carlo – The International Association of Athletics Federations (IAAF) announced Monday it was hacked by the hacker group Fancy Bear, which the US has previously linked to Russia. The IAAF stated that the hack compromised athletes' therapeutic use exemption applications (TUEs), which provide special exemptions to athletes for use of otherwise banned substances for a specific medical need. The IAAF also said "the presence of unauthorized remote access to the IAAF network by the attackers was noted on 21 February where meta-data on athlete TUEs was collected from a file server and stored in a newly created file." While the IAAF did not know if any data was taken, it said there was "a strong indication of the attackers' interest and intent."
SOURCE: 3 April 2017, NBC News

(U) North Korea – Link Found to Cyber Heist

(U) Pyongyang – Cyber security firm Kaspersky has possibly linked North Korea to the $81 million cyber heist of the Bangladesh central bank account at the Federal Reserve Bank of New York. Kaspersky released a report that links the hacker group Lazarus, which carried out both the cyber heist and the 2014 hack on Sony's Hollywood Studios, to an IP address in North Korea. It is currently unclear if Lazarus was working with people from North Korea or if the country sponsored the attack. The cyber heist was one in a string of recent attacks by Lazarus targeting financial institutions.
SOURCE: 3 April 2017, Reuters

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLESE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-874-1100.

Warning: This document is the exclusive property of the State Threat Assessment Center (STAC) and is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the California Public Records Act (Govt. Code Sec. 6250-6270). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with STAC policy relating to U//FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized STAC official. No portion of this report should be furnished to the media, either in written or verbal form.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.